Пятый Международный Информационный Форум по аналитическим методам и компьютерным кодам оценки безопасности атомных станций с реакторами типа ВВЭР и РБМК
16-20 Октября 2000, г. Обнинск, Россия

ПРОГРАММНЫЙ ИНСТРУМЕНТАРИЙ ДЛЯ КОНТРОЛЯ И УЛУЧШЕНИЯ ПОКАЗАТЕЛЕЙ ЭКСПЛУАТАЦИОННОЙ БЕЗОПАСНОСТИ АЭС

Малкин С.Д., Сивоконь В.П, Позняков В.В., Гладышев М.Е.
Российский Научный Центр "Курчатовский Институт",
123182, Россия, Москва, пл. Курчатова д.1
эл. почта: sivla@dcmm.kiae.ru

Ключевые слова: Эксплуатационная безопасность, обратная связь, Культура Безопасности, надежность, инструментарий самооценки.

Доклад посвящен программному инструментарию **ACCET** (**A**ssessment of **C**onsequences and **C**auses of **E**vents **T**ool - Инструментарий Оценки Последствий и Причин Нарушений), его последним модификациям и опыту использования, особенно для контроля эксплуатационных показателей и Культуры Безопасности (КБ) АЭС. В частности, показывается реальная (базирующаяся на эксплуатационных данных) эффективность внедрения тренажеров на ВВЭР и РБМК. Первая версия инструментария была разработана в сотрудничестве с МАГАТЭ и полностью основана на методе ASSET (программа **ERCATD**). В течение 1997-1999 различные АЭС в Финляндии, Казахстане, России и Украине, при самооценке их эксплуатационной эффективности, успешно апробировали инструментарий, делая акцент на Культуре Безопасности (КБ). Опыт, накопленный на этих станциях, обсуждения на семинарах позволили придти к следующим заключениям. 1) Реальные текущие проблемы станции могут быть определены и отслежены только путем непрерывного анализа данных по всем эксплуатационным отказам, даже маленьким отклонениям и промахам. 2) Все эксплуатационные отказы могут быть полностью идентифицированы в процессе разработки Логического Дерева Отказов (ЛДО), с последующим анализом причин доминирующих отказов. 3) Регулярная самооценка эксплуатационных показателей АЭС с применением программного инструментария **ACCET** является действенным методом для своевременного обнаружения и исправления нерешенных проблем безопасности, надежности и КБ, также как и для контроля тенденций изменения эксплуатационных характеристик систем КИП, персонала и всей станции. Доказано, что эффективность инструментария **ACCET** для контроля эксплуатационных показателей может быть значительно повышена за счет модификаций, выходящих за рамки первоначального подхода. Среди главных изменений – оценка всех потерь, внедрение интегрированного контроля характеристик станционных систем и автоматизированное управление корректирующими действиями, модификация инструментария для существующей локальной практики. Модифицированный инструментарий был установлен и успешно используется на финской АЭС **Olkiluoto** (IAEA-TECDOC-1125, Декабрь 1999).

Пятый Международный Информационный Форум по аналитическим методам и компьютерным кодам оценки безопасности атомных станций с реакторами типа ВВЭР и РБМК
16-20 Октября 2000, г. Обнинск, Россия

SOFTWARE TOOL FOR PLANT OPERATIONAL SAFETY PERFORMANCE MONITORING AND ENHANCEMENT

S.Malkin, **V.Sivokon,** V.Pozniakov, M.Gladyshev

Russian Research Centre "Kurchatov Institute",
123182, Kurchatov sq., Moscow, Russia
E-mail: sdm@dcmm.kiae.ru**; E-mail: sivla@dcmm.kiae.ru**

Keywords: Operational safety performance, Operating feedback, Safety Culture, Reliability, Self-assessment tool.

ABSTRACT

The paper presents **ACCET** software tool (Assessment of Consequences and Causes of Events Tool), its recent development and usage experience, especially as for NPP I&C and personnel performance monitoring. In particular, it shows real (based on operational data) efficiency of the simulators implementation at WWER and RBMK Units. **ERCATD** code - the first version of the **ACCET** software tool was developed in co-operation with IAEA and fully based on IAEA ASSET method. During 1997-1999 in Kazakhstan, Russia, Ukraine and Finland several nuclear power plants while self-assessing operational performance of their equipment, personnel and procedures successfully tested the tool with accent to Safety Culture (**SC**). The experience accumulated at these plants and discussions at the seminars allowed achieving the following conclusions. 1) Plant current status of safety and reliability problems can only be identified and monitored based on permanent analysis of the safety impact, nature and causes of all the operational failures, even small deviations. 2) All operational failures (occurrences) could be fully identified in the process of Logic Tree of Occurrences (LTO) establishing followed by occurrences analysis. 3) Regular self-assessment of operational performance with the help of **ACCET** is an effective method for timely detection and elimination of any pending safety, reliability, **SC** problems and monitoring the trends of I&C, personnel and overall plant operating performance. It has been proven that an effectiveness of **ACCET** for plant systems (especially personnel) performance monitoring could be significantly enhanced by the modifications, which are beyond original ASSET approach. The modified tool was installed and successfully being used at Finnish NPP **Olkiluoto** (IAEA-TECDOC-1125, December 1999).

1. INTRODUCTION

The first version of the **ACCET** software tool, running under MS Windows' control, was developed in co-operation with IAEA in the end of 1996. It was fully based on IAEA ASSET method, which has been mainly developed by Bernard Thomas in assistance with colleagues [1, 2]. Historically and logically the **ACCET** became the further development of ASSETAS software, designed earlier in DOS environment [3]. The main idea of the **ACCET** is analysis of the event causes by answering thoroughly the

questions, listed in **Table 1**. The key question among them is "Why were the problems not prevented?" This is the way to find the root cause of any safety problem and weaknesses of the plant defence in depth. The main **ACCET** reports and statistical data, supporting answering the questions, are presented in the same table. The tool can automatically create them, detailed information is provided in manual [4].

Table 1. ACCET brief guidance for self-assessment of plant safety performance

7 BASIC QUESTIONS	ACCET main reports	ACCET calculated data
WHAT ARE THE PENDING SAFETY PROBLEMS?	• Recurrent Failures and Safety Problems • Pending Safety Problems Analysed	• Nature of Failures (I&C, (Procedures, Personnel, etc.)
HOW IMPORTANT ARE THEY? (Significance)	• Event Rating Form • Safety Functions Impacted • Problems Significance to Safety • Problems Significance to Safety Culture • Problems Significance to Production & Availability	• Safety Attributes • Events Significance • Number of Events Reported • Significance of the safety problems
WHY DID THEY HAPPEN? (Direct Causes)	• Logic Tree of Occurrences (Failures) • Problems Dominant Failures • Event Root Cause Analysis Form (ERCAF, part 1) • Direct Causes of Dominant Failures	• Nature of Failures • Events Discovered by Surveillance • Dominant Causes (Direct)
WHY WERE THEY NOT PREVENTED? (Root Causes)	• ERCAF, part 2 • Root Causes of Dominant Failures • Table of Self-Assessment	• Dominant Causes of Events (Root)
HOW TO ELIMINATE THE PENDING SAFETY PROBLEMS? (Repairs)	• ERCAF, part 3 • List of Corrective Actions (1) • Table of Self-Assessment	• Corrective Actions Data (part 1)
HOW TO PREVENT THEIR RECURRENCE? (Remedies)	• ERCAF, part 4 • List of Corrective Actions (2) • Table of Self-Assessment	• Corrective Actions Data (part 2)
WHAT CORRECTIVE ACTIONS SHOULD STILL BE IMPLEMENTED? (Action plan)	• Action Plan • Corrective Actions (CA) Management	• On-line monitoring "Top ten" of CA

During 1997-1999 the tool was successfully tested by Balakovo, Leningrad, Smolensk (Russia), Olkiluoto (Finland), Aktau (Kazakhstan), Rovno, Chernobyl and South-Ukrainian (Ukraine) nuclear power plants while self-assessing operational

performance of their equipment, personnel and procedures with accent on **SC**. A lot of modifications have been implemented based on the operational feedback and new ideas of the tool designers. Among them:

- Extension of the causes analysis for all the events reported, even small deviations ("Out of scale" events, INES);
- Taking into account all impacts of the event, including production and availability losses, significance to safety and **SC**;
- Engineering interpretation of the **SC** definition and implementation of the extended set of indicators for integrated monitoring plant operational performance;
- Realisation of corrective actions computerised management with on-line monitoring the "top ten" actions;
- Adjustment of the tool to the local management practice and reporting system.

The next chapters describe the latest state of the tool methodological background and the complete set of indicators, suggested for integrated monitoring of plant systems operational performance, including operational safety, reliability and **SC** monitoring.

2. MAIN METHODOLOGICAL ASPECTS

In accordance with "Basic Safety Principles for Nuclear Power Plants" (№75-INSAG-3) the fundamental safety objective is to prevent accidents, based on comprehensive defence in depth including sound **SC** as an important element of plant defence in depth. **Safety Culture definition** (№75-INSAG-4): **SC** is that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, nuclear plant safety issues receive the attention warranted by their significance.

The **ACCET** gives clear and logical answer how to assess all the aspects highlighted above. The diagram in **Fig. 1** explains the general mechanism of the latent weakness influence on the plant operation [3]. With the help of this diagram it could be easily shown, what is needed from the plant management to control the situation at the plant and to provide plant operation as safe and reliable as possible. There is no ideal plant in the World. Latent weaknesses exist in all the areas relevant to plant operation: equipment, personnel and procedures. The latent weaknesses are developing into the failures and further into the events, leading to the deviations of the plant normal operation. In accordance with the defence in depth approach there should be several layers to protect the plant: hardware (safety barriers and systems), software (personnel, procedures) and management (**SC** at the level of the organisation/plant). As it is shown in **Fig. 1**, from the engineering point of view, the last layer - **SC**, could be split on three main sub-layers or **SC** layers, based on the **SC** definition, given above. From the first look the last **SC** layer (**Capability of learning the lessons)** may show oneself insignificant as compared with the first two. Really, if the two first **SC** layers are effective enough, at the third layer we can see recurrent events of low level of significance only. That is true, but however still potentially dangerous as the recurrent events, having the same causes (not eliminated because they are recurrent), next time may appear with much more severe consequences.

All three **SC** layers can be assessed and monitored by cause analysis of the events, calculation and trending the proper indicators. Simultaneously, overall plant operational performance, including safety and reliability, could be monitored.

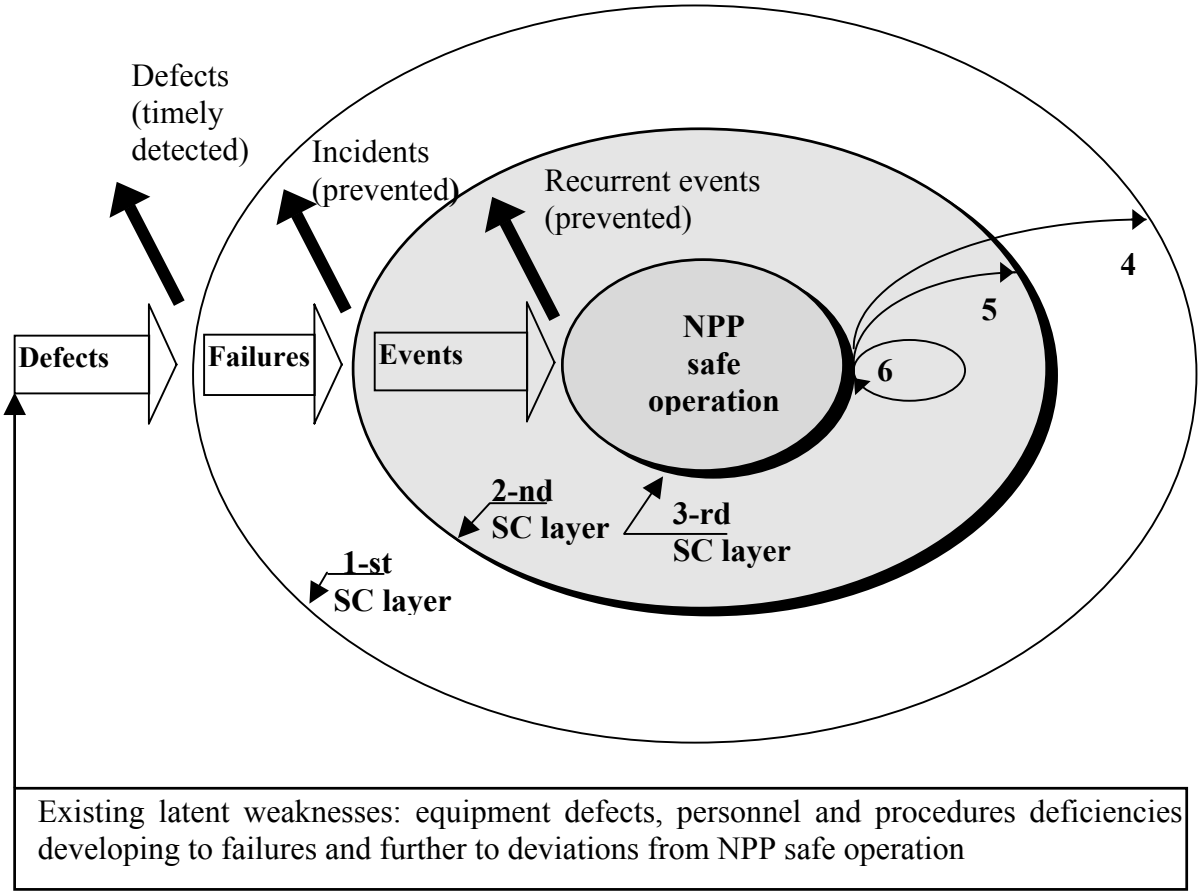


Fig. 1. ACCET mechanism of NPP safe operation disturbance, based on engineering interpretation of Safety Culture definition:
1-st SC layer (1-st aspect of Safety Culture): Identification of the latent weaknesses by: 1 - quality control, 2 - preventive maintenance and 3 - management surveillance for unforeseen degradation (Capability to identify the latent weaknesses and pending safety problems). **2-nd SC layer** (2-nd aspect of Safety Culture): Prevention of incidents and accidents, holding of the events at the lowest level of significance (Capability to assess and reduce significance of the events/problems and to respond to them adequately: priority, timely reaction, redundancy). **3-rd SC layer** (3-rd aspect of Safety Culture): The event root cause analysis and development of effective corrective actions (Capability of learning the lessons from operational experience and elimination of the safety problems). **4, 5, 6 -** Feedback to enhance all 3 aspects of Safety Culture.

To find the most informative indicators, which have to be based on the facts - real events from the operational history, the following procedure of the event analysis was implemented:

- Identification of the event, its description and data on safety impact, production losses and how it was discovered;
- Assessment of the event significance, based on INES or similar approach, and safety function or barrier impacted during the event sequence;
- Establishing the **LTO** for each event with identification of the nature of all the dominant occurrences (failures);
- Root cause analysis of the dominant failures with detection of all the **SC** aspects;

- Identification of the families of the recurrent failures, based on safety functions/barriers impacted and nature of the failures with calculation of their significance to safety, production and **SC**;
- Calculation of the indicators.

Since the beginning of 90-th, ASSET recommended calculation of several integral indicators for the operational performance monitoring. Then, in the end of 1997, Bernard Thomas introduced **Safety Culture Scale (SCS)** for assessing individual event and we may call its criteria **SC** event-individual indicators [4]. To complete the indicators set a new group of so-called differential indicators was proposed [3] for integrated monitoring of the plant operational performance, including simultaneous monitoring of operational safety, reliability and **SC**.

3. INDICATORS FOR INTEGRATED MONITORING THE PLANT OPERATIONAL PERFORMANCE

Based on the methodological background described above, the following set of three complementary groups of the indicators are suggested:

- integral indicators, based on the all population of the events;
- differential indicators, based on pre-defined groups of events;
- event-individual indicators based on comparison of the each individual event data with the plant operational history by the use of the **SCS**.

Integral indicators. The first two of them are being used since long time for operational safety performance assessment and they could be used for plant **SC** assessment as well, the third indicator was proposed later [3, 4]:

1) **Capability of identifying the latent weaknesses (or Efficiency of surveillance)** is defined by calculation of the ratio between number of events discovered by surveillance and total number of the events.
2) **Capability of assessing and reducing events significance (or Efficiency of incidents prevention)** is defined by calculation of the ratio between number of events with low level of significance and total number of the events.
3) **Capability of learning the lessons (Efficiency of recurrent events prevention)** is defined by calculation of the ratio between number of non-recurrent events (out of families of recurrent failures) and total number of the events.

Differential indicators. This new group of the indicators is being implemented in the **ACCET**. The idea is to monitor all three integral indicators (1, 2, and 3) together with their cuts per the main types of the plant systems. For example, we used to consider the following plant systems: Equipment (Mechanical, Electrical and I&C), Personnel and Procedures (Operating and Maintenance). Corresponding indicators, let us call them differential indicators, may help to monitor the plant **SC** and systems operational performance at the relevant shop level. Comparison of integral indicator with the differential indicators, calculated for pre-set groups of equipment very often shows that operational performance trends in some groups of equipment may significantly differ from the general trends monitored by integral indicators. Events for each pre-defined group could be automatically extracted from the total population of the events by the **ACCET**. Such differential indicators could be useful for the plant systems reliability monitoring as well. In that case, not only relative values of the indicators, but also absolute numbers of failures of different systems should be monitored. For the plant systems reliability monitoring it is also recommended to split the groups of equipment on sub-groups covering the elements of the same type, like Detectors, Transmitters, Regulators for I&C, etc.).

Event-individual indicators. These indicators are fully based on **SCS**. The **SCS** implementation has arisen from the idea of comparison of each event data with the plant operational history, because each event carries useful information for **SC** assessment provided existence of any basis for such comparison. In spite of the fact that exact contents of **SCS** could be assessed as discussible, the scale application is undoubtedly useful. It gives the tool for **SC** assessment from each new event analysis, without waiting the statistically adequate data to calculate the integral or other statistical indicators.

4. ACCET DESCRIPTION AND IMPLEMENTATION EXPERIENCE

ACCET contains two parts: The main part (ERCATD) is meant to help Users answering on 7 basic questions of **ACCET** self-assessment (**Table 1**). It is the tool and database, written in MS Access 2.0 and converted to MS Access 2000. Another part (INESAR for Windows) is meant to help Users with application of the INES procedures of event consequences rating. It is written in C++ and could be used either with **ACCET** or separately. **ACCET main functions** are the following:

- computerised input of all needed information on operational events in accordance with self-assessment guidance (**Table 1**);
- computerised assessment of the events significance according to INES procedures;
- accumulation of the information and use it for the analysis of the events causes and nature, **SC** aspects, assessing sufficiency of the offered corrective actions;
- processing and analysis of statistical data on events for learning appropriate lessons and improvement of NPP management;
- calculation and trending the set of the indicators for integrated monitoring of the plant operational safety, reliability and **SC**;
- automatic generation of the documents, including standard self-assessment forms;
- graphic presentation of the event statistical data in the various forms;
- evident learning the self-assessment procedures.

During 1997-1999 various NPPs in Finland (Olkiluoto NPP), Russia (Balakovo, Leningrad and Smolensk NPPs) and Ukraine (Chernobyl, Rovno and South-Ukraine NPPs), while self-assessing their operational performance, successfully tested the tool with an accent on Safety Culture. The latest **ACCET** version has been developed in Finnish for Olkiluoto NPP. It was adjusted to existing local practice of management and reporting. Such "localisation" could be recommended for the other plants. As the result of **ACCET** (and ASSET before 1997) approach implementation, the plant operational safety and efficiency have been significantly improved almost everywhere without heavy investments in additional equipment [2, 3]. As the example of the significant progress achieved after the method implementation at the plant one may refer to the Balakovo NPP (4 Units of WWER-1000) and Russian plants in general. Balakovo NPP is conducting ASSET/**ACCET** assessment since 1992 and on the annual basis since 1996. Number and significance of the events have been significantly decreased, including ones with the personnel failures, **Fig. 2.**

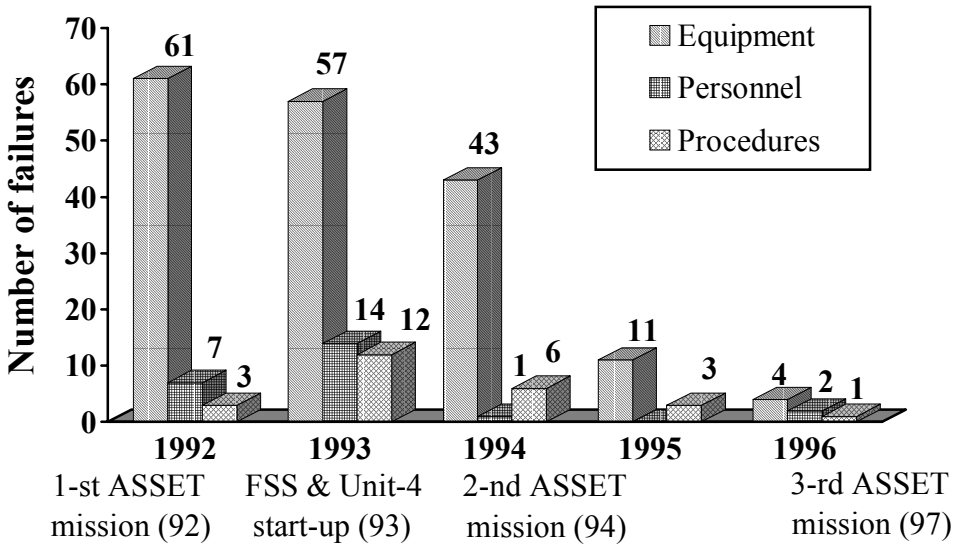


Fig. 2. Type and number of Balakovo NPP failures per years during last period of ASSET monitoring (data based on safety relevant events)

The last result was also caused by Training Centre organisation with **Full-Scope Simulator (FSS)** implementation. It has been shown by **ACCET** that implementation of simulators at other WWER and RBMK gave the same stable effect besides, may be, the first RBMK-**FSS** implementation at Smolensk NPP in 1989. Computers used in this **FSS** were not powerful enough to reach adequacy of all dynamic models. That is why the **FSS** was not satisfactory effective as it was clearly shown by ASSET monitoring and has been fully redesigned later. To explore good practice of ASSET/**ACCET** usage in 1999 WANO considered possibility to use the ASSET self-assessment for the plants of Paris Centre [5]. The experience accumulated at the plants, listed above, and discussions at the seminars in Bulgaria, Canada, Lithuania, Kazakhstan, Romania, Russia, Sweden, UK, Ukraine and other countries show the following.

Plant current status of safety, reliability and Safety Culture problems (I&C, personnel and etc.) can only be identified and monitored based on permanent analysis of the safety impact, nature and root causes of all the operational failures, even small deviations and near misses. Causes analysis of safety relevant events only, which was recommended in the past, limits the basis of learning the lessons especially for the plants with good performance (a few safety relevant events per year). All operational failures (occurrences) could be fully identified in the process of **LTO** establishing followed by dominant occurrence nature and causes analysis. Experience of event analysis has shown that without thinking on **LTO** it is hardly possible to reveal all the failures in the consequence of the event. There are many examples when event was caused by coincidence of several different occurrences, which are not fully visible from the event description, especially personnel and procedures failures. So, **LTO** establishing gives personnel possibility to identify all the event failures, but not the event logic only. For example, event "Release of 20 m3 of low radioactive water on turbine hall roof due to lack of maintenance work verification" (Kalinin NPP Unit-1, 1990) occurred because:

- During short circuit a fuse failed to open control circuit (maintenance personnel installed wrong fuse) followed by failure of emergency busbar №3;

- DG-1 cooling has independently failed to maintain oil temperature within OL&C followed by DG-1 failure (emergency busbar №3 failure);
  (Then Unit-1 cooling down was started up due to loss of two emergency busbars)
- The indicator of water level in SG-4 failed to give correct information followed by ingress of feedwater into steam line;
- All the SGs of Unit-1 failed to be tight (tube leakage);
- Operating personnel failed to follow normal cooldown mode and used relief valve to atmosphere (BRU-A).

The last failure is not obvious as procedure allows several ways of WWER cooldown.

5. CONCLUSION

Real current status of the plant weaknesses, its safety, reliability and **SC** problems can only be identified and monitored based on the permanent analysis of all operational failures, even small deviations. All the failures could be hardly identified without thinking on the **LTO** establishing for each event and analysis of its failures.

Regular plant self-assessment of operational performance based on the event analysis is an effective method for timely detection and correction of the weaknesses, any pending problems and monitoring the trends of I&C, personnel and overall plant performance. Safety, reliability, **SC** and plant efficiency could be significantly improved everywhere without heavy investments in additional equipment. **ACCET**, which contains the complete set of the integral, differential and event-individual indicators for integrated monitoring the plant operational performance, including safety, reliability and **SC** monitoring, became the practical tool, which is useful for the plant self-assessment. It could be easily adjusted to the plant local practices of the management and reporting, as it was shown for Olkiluoto NPP [6].

REFERENCES

1. Thomas, B., 1996. ASSET celebrates 10 years anniversary. *IAEA bulletin*, v. 38, **4**, pp.39-40.
2. Reisch F., Bliselius P., 1998. IAEA-ASSET evaluating NPP safe performance. *Nuclear Europe Worldscan*, **1-2**, pp. 66-67.
3. Sivokon V., 2000. From General Approach to Practical Tool for Integrated Monitoring of the Operational Performance of Nuclear Power Plants. Proc. IAEA Specialists' Meeting on Integrated Information Presentation in Control Rooms and Technical Offices at Nuclear Power Plants, 9-12 May 2000, Stockholm, to appear.
4. Thomas B., 1985-2000. *Plant Self-Assessment. User's Manual (To Enhance "Accident Prevention")*. IAEA, Vienna.
5. Self-assessments: WANO Paris Centre is looking at new ways to offer assistance to utilities in making more effective use of Operating Experience, 1999. *Inside WANO*, **20**, p.13.
6. IAEA-TECDOC-1125. Self-assessment of operational safety for nuclear power plants, Vienna, December 1999, p.96-97.

SAS Lab

Пятый Международный Информационный Форум по аналитическим методам и компьютерным кодам оценки безопасности атомных станций с реакторами типа ВВЭР и РБМК

16-20 Октября 2000, г. Обнинск, Россия

ПРОГРАММНЫЙ ИНСТРУМЕНТАРИЙ ДЛЯ КОНТРОЛЯ И УЛУЧШЕНИЯ ПОКАЗАТЕЛЕЙ ЭКСПЛУАТАЦИОННОЙ БЕЗОПАСНОСТИ АЭС

SOFTWARE TOOL FOR PLANT OPERATIONAL SAFETY PERFOMANCE MONITORING AND ENHANCEMENT

Малкин С.Д., Сивоконь В.П, Позняков В.В., Гладышев М.Е.

S.Malkin, V.Sivokon, V.Pozniakov, M.Gladyshev

Russian Research Centre “Kurchatov Institute”,

123182, Kurchatov sq., Moscow, Russia

E-mail: **sivla@dcmm.kiae.ru,** sdm@dcmm.kiae.ru

SAS Lab

ACCET Management Support System

SAFETY
(INSAG-3 - BASIC SAFETY OBJECTIVE)

FUNDAMENTAL SAFETY OBJECTIVES:

NO ACCIDENT

IS MET BY DEPLOYMENT OF AN EFFECTIVE

DEFENCE IN DEPTH

WITH SOUND

SAFETY CULTURE

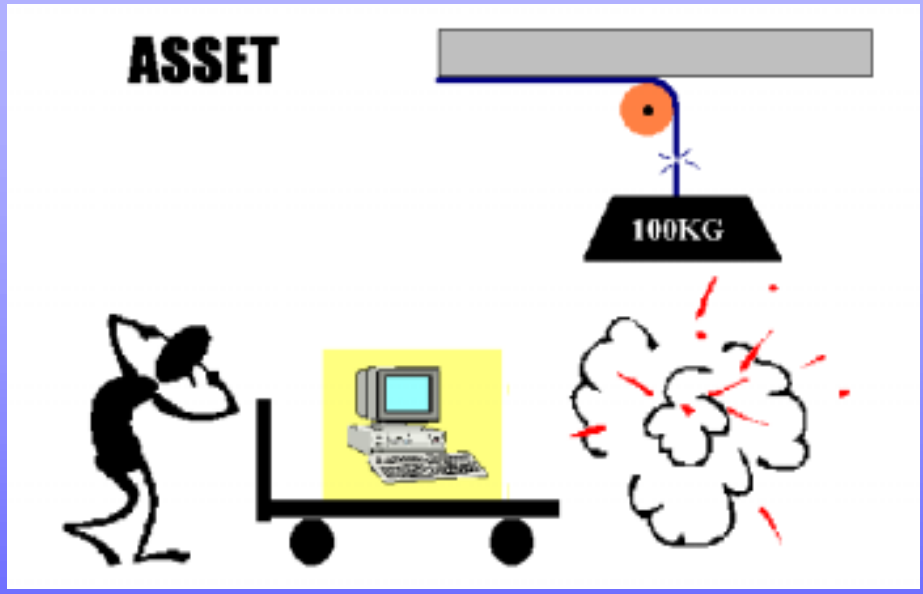
AS IMPORTANT

D-in-D SAFETY LAYER

COMPLEMENTARY TO NPP HARDWARE AND SOFTWARE PROVISIONS

SAS Lab

Learning from Deviations to Prevent Accidents



THE CONSEQUENCES MAY BE DIFFERENT:

–**DEVIATION** (LOAD DROPPED)

–**INCIDENT** (COMPUTER BROKEN)

–**ACCIDENT** (WORKER INJURED)

THE CAUSES ARE THE SAME:

1. WHY DID IT FAIL? (DIRECT CAUSE)

DEGRADED CABLE NOT IDENTIFIED BY QUALITY CONTROL PRIOR TO OPERATION
OR
DEGRADATION OF CABLE NOT ADDRESSED BY PREVENTIVE MAINTENANCE

2. WHY WAS IT NOT PREVENTED? (ROOT CAUSE)

DEGRADED CABLE NOT DETECTED BY PERIODIC TESTING (SURVEILLANCE POLICY)
OR
DEGRADED CABLE NOT RESTORED (FEEDBACK POLICY)

DUE TO QUALITY CULTURE DEFICIENCY

SAS Lab

Software Tool "ACCET"

"ACCET":

Analysis of Consequences and Causes of Event Tool

Consequences (Severity) :
"INESAR for Windows" Code
(INES Automated Rating)

Causes (Direct & Root):
"ERCATD" Code
(Event Root Cause Analysis Tool and Database)

Code *"INESAR for Windows"*
Written: Borland C++
Requires: 2 MB RAM Memory
1 MB Hard Disk Mem.
Windows 3.11, 95, 98
Developed: SAS Lab, Moscow
Copyright: SAS Lab, Moscow
Last version: 1996

Code *"ERCATD"*
Written: MS ACCESS
Requires: 6 MB RAM Memory
5 MB Hard Disk Mem.
Windows 3.11, 95, 98
Developed: SAS Lab, Moscow
Copyright: IAEA, Vienna
Last version: June 1997
(new ERCATD-Fin January 2000)

Contact persons:

Bernard Thomas IAEA, Vienna
(phone +43 1 2600 22685, fax +43 1 2600 29723)
Vladimir Sivokon, SAS Lab, RRC "Kurchatov Institute" Moscow
(phone +7 095 1969378, fax +7 095 1968891)

SAS Lab

Safety Culture Engineering Interpretation

1-st ASSET layer (1-st aspect of Safety Culture)

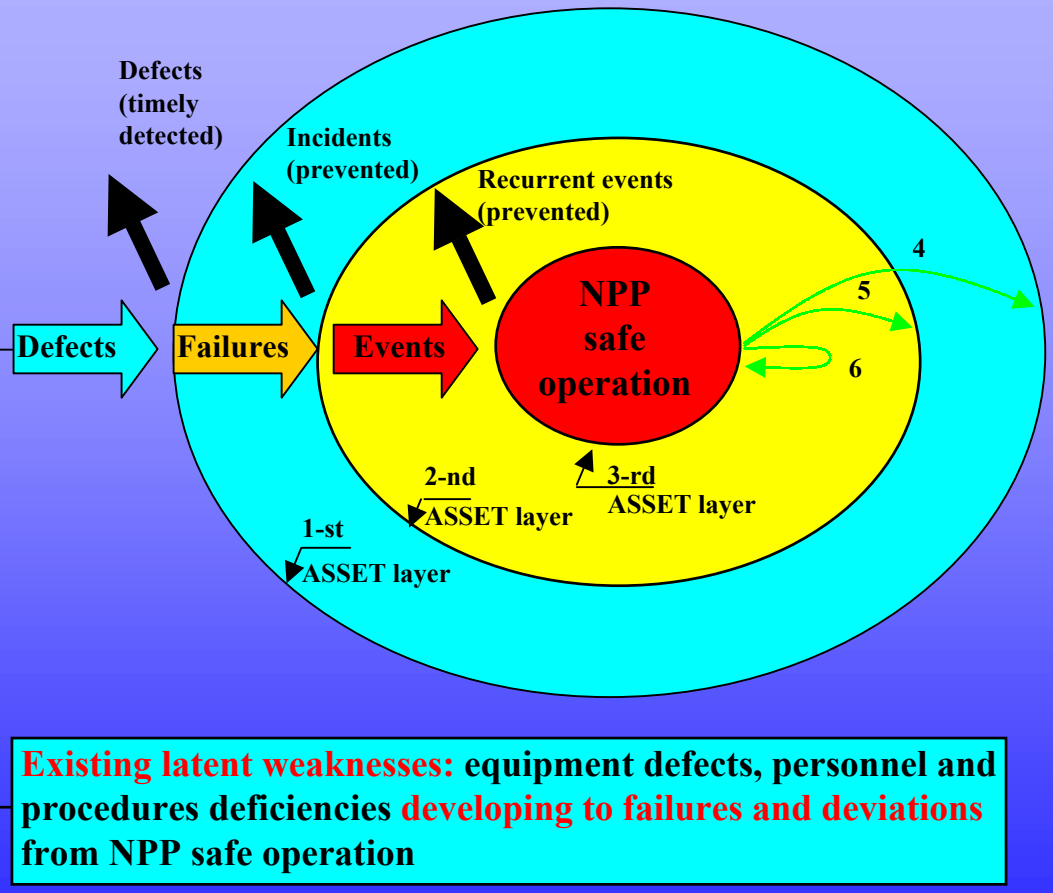
Identification of the latent weaknesses by: **1 - Quality Control, 2 - Preventive Maintenance and 3 – Surveillance Testing (Capability to identify the latent weaknesses and pending safety problems)**

2-nd ASSET layer (2-nd aspect of Safety Culture)

Prevention of incidents and accidents, holding of the events at low level of significance (**Capability to assess significance of the events, safety problems and to respond to them adequately: fault tolerance, priorities, timely reaction**)

3-rd ASSET layer (3-rd aspect of Safety Culture)

The event root cause analysis and development of effective corrective actions (**Capability of leaning the lessons from experience and elimination of recurrent events and safety problems**)



4, 5, 6 - Feedback to enhance all the 3 aspects of Safety Culture

SAS Lab

Integral Indicators

Capability of identifying the latent weaknesses (Efficiency of surveillance):

$$I_1 = \frac{N_{DS}}{N} \times 100\%$$ (or equivalent); **(1)**

where: **N**>0 – total number of event reported inside and outside the plant;
N_{DS} –number of events **D**iscovered by **S**urveillance.

Capability of assessing events significance (Efficiency of incidents prevention):

$$I_2 = \frac{N_{LL}}{N} \times 100\%$$ (or equivalent); **(2)**

where: N_{LL} – number of the events having **L**ow **L**evel of significance (“Out of scale” or “Out of scale” together with events rated by “0”, INES).

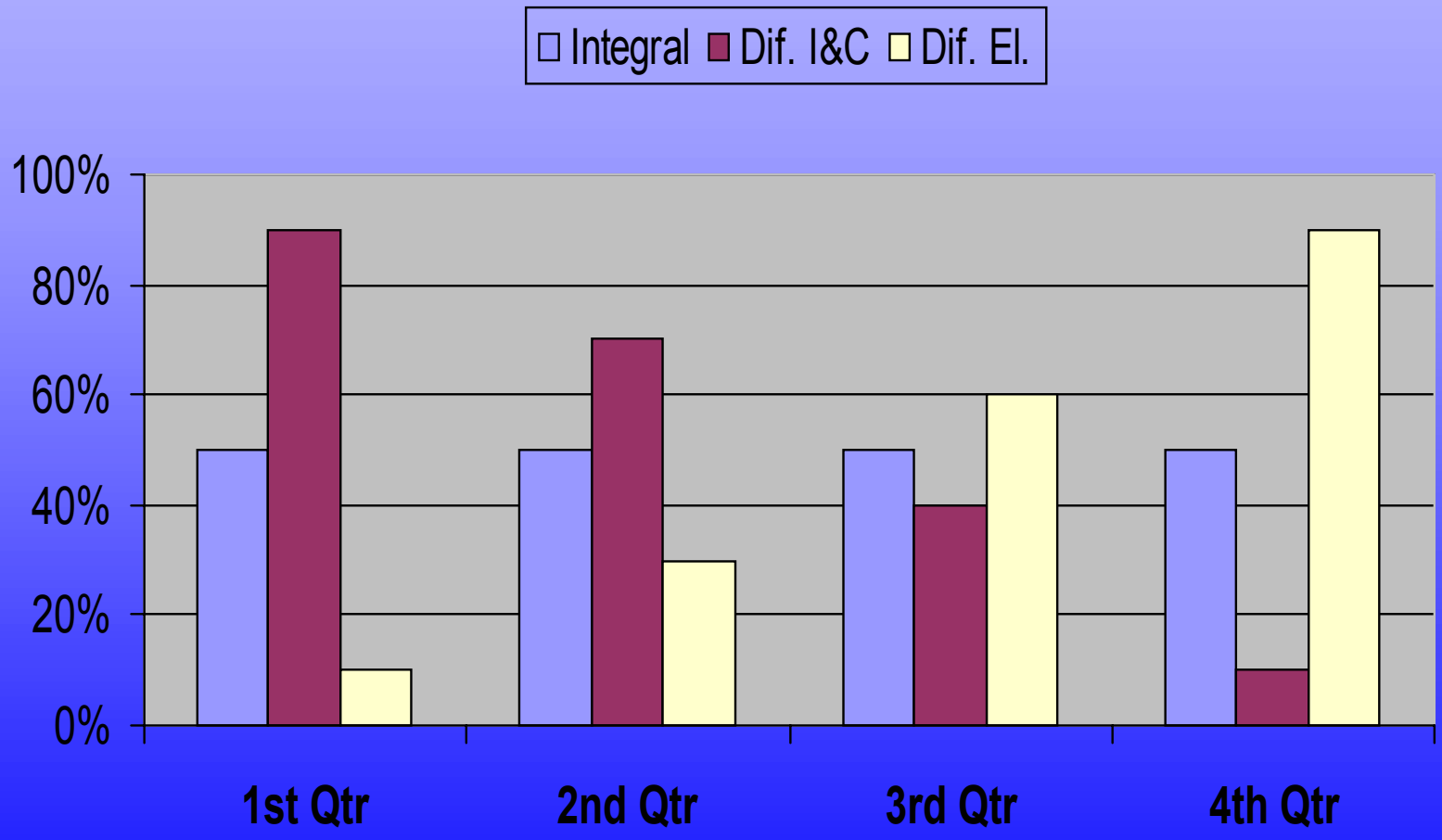
Capability of learning the lessons (Efficiency of recurrent events prevention):

$$I_3 = \frac{N_{NR}}{N} \times 100\%$$ (or equivalent); **(3)**

where: N_{NR} – number of the events, which are **N**ot **R**ecurrent (outside the families of the recurrent events).

SAS Lab

Comparison of Integral Indicator with the Differential Indicators, Calculated for I&C and Electrical Equipment



SAS Lab

ACCET Guidance for Plant Self-Assessment of Safety Performance

N	ASSET 7 BASIC QUESTIONS	ACCET code main reports	ACCET code statistics
1	WHAT ARE THE PENDING SAFETY PROBLEMS?	• Recurrent Failures and Safety Problems • Pending Safety Problems Analysed	• Nature of Failures (Personnel, Procedures, I&C, etc.)
2	HOW IMPORTANT? (Significance)	• ERF • Safety Functions Impacted • Problems Significance to Safety • Problems Significance to Production & Availability	• Safety Attributes • Events Significance • Number of Events • Significance of the safety problems
3	WHY DID THEY HAPPEN? (Direct Causes)	• LTO • Problems Dominant Failures • ERCAF • Direct Causes of Dominant Failures	• Nature of Failures • Events Discovered by Surveillance • Dominant Causes
4	WHY WERE THEY NOT PREVENTED? (Root Causes)	• ERCAF, part2 • Root Causes of Dominant Failures • Table of Self-Assessment	• Dominant Causes of Events (Root)
5	HOW TO ELIMINATE THE PENDING SAFETY PROBLEMS? (Repairs)	• ERCAF, part 3 • List of Corrective Actions (1) • Table of Self-Assessment	• Corrective Actions Data (part 1)
6	HOW TO PREVENT THEIR RECURRENCE? (Remedies)	• ERCAF, part 4 • List of Corrective Actions (2) • Table of Self-Assessment	• Corrective Actions Data (part 2)
7	WHAT CORRECTIVE ACTIONS SHOULD STILL BE IMPLEMENTED? (Action plan)	• Action Plan • Corrective Actions (CA) Management	• On-line monitoring “Top ten” of CA

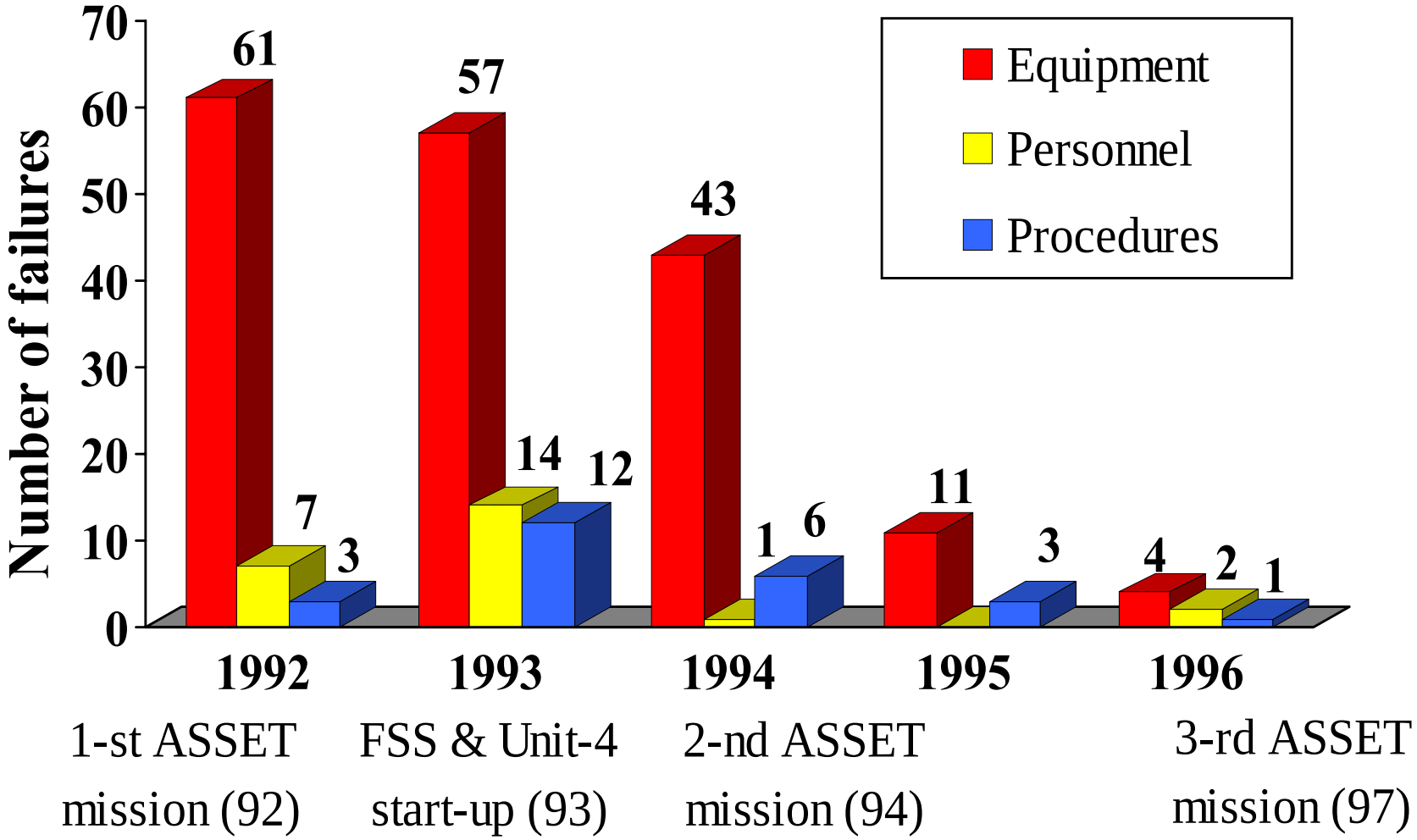
SAS Lab

ERCATD-E (R, F ...) Modernisation in English (Russian, Finnish ...)

N	MODERNISATION TASK DESCRIPTION	OBJECTIVES
1	**Adjustment of the software to the latest ASSET guidance**	• Implementation of **Safety Culture Scale** • **Extension and enhancement of the main tables** • **Extension of events analysis up to the all events reported** • **Implementation of new tables**
2	**New functions implementation**	• **Corrective actions computerised management** • **ACCET self-checking of LTO creation** • **Integrated monitoring of plant operational performance, reliability and SC**
3	**Software localisation oriented on particular customer**	• Translation into **local languages** (R, F, S) • Implementation of new functions, tables and reports • Identification of all the by NPP name • **Customised maintenance**
4	**Y2K Problem**	• **Right identification of 2000 year**
5	**Adjustment of the software to new MS Office (Access 2000)** (DONE for Finnish version, PENDING for English version, as of 01.03.2000)	• **On-line spelling** • **Reports saving and view (Snapshot)** • Hyperlinks in MS Office documents • Saving on HTML • Removable source code

SAS Lab

Balakovo NPP Failures During Last Period of ASSET Monitoring



SAS Lab

Main Conclusions

- Real current status of the plant's safety, reliability and **SC** problems can only be identified and monitored based on the permanent analysis of all operational failures, even small deviations.

- All the failures could be hardly identified without thinking on the logic of each event and analysis of its failures.

- Regular self-assessment of plant operational performance based on the event analysis is an effective method for timely detection and correction of the pending problems, monitoring the trends of overall plant performance. Safety, reliability, **SC** and plant efficiency could be significantly improved everywhere without heavy investments in additional equipment.

- **ACCET**, which contains the complete set of the integral, differential and event-individual indicators for integrated monitoring the plant operational performance, including safety, reliability and **SC** monitoring, became the practical tool, which is useful for the plant self-assessment. It could be easily adjusted to the plant local practices as it was shown for Olkiluoto NPP in Finland.